

**BY ORDER OF THE SECRETARY
OF THE AIR FORCE**

AIR FORCE POLICY DIRECTIVE 10-7

4 AUGUST 2014



Operations

INFORMATION OPERATIONS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This AFPD is available for downloading from the e-Publishing website at www.e-Publishing.af.mil

RELEASABILITY: There are no releasability restrictions on this publication

OPR: AF/A3O-QI

Certified by: HQ AF/A3/5
(Lt Gen Burton M. Field)

Pages: 18

Supersedes: AFPD10-7, 6 September 2006;
AFPD10-11, 31 May 2001;
AFPD10-20, 1 October 1998

This policy directive implements DoDD 3600.01, Information Operations (IO), 2 May 2013; DoDD S-3321.1, Overt [MISO] Conducted by the Military Services in Peacetime in Contingencies Short of Declared War; DoDI S-3604.01, DoD Military Deception (MILDEC), 11 March 2013; DoDD 5205.02E, DOD Operations Security (OPSEC) Program, 20 June 2012; DoDI 3608.11, Information Operations Career Field, 4 November 2005, directing the establishment of IO professional development boards in each Military Service; and DoDI 3608.12, Joint IO Education, Change 1, 6 December 2011, assigning responsibilities within the Air Force for Joint IO education and providing guidance for planning and conducting Air Force Information Operations (IO) to support the warfighter and achieve national strategy objectives. This policy applies to all military and civilian Air Force personnel, members of the Air Force Reserve, Air National Guard, DoD contractors, and individuals or activities under legal agreements or obligations with the Department of the Air Force. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS).

SUMMARY OF CHANGES

This change incorporates the 20 February 2014 administrative and substantive changes to AFPD 10-7. These changes deletes obsolete references and updates office symbols and publication dates; implements DoDD 3600.01, Information Operations (IO), 2 May 2013, directing fundamental change in the definition of IO; and includes administrative and policy changes from HQ USAF.

1.	Introduction.	2
2.	General.	3
3.	Responsibilities.	4
4.	See Attachment 1 for references and supporting information.	12

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 13

1. Introduction. IO is the integrated employment, during military operations, of information-related capabilities (IRCs) in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. The definition emphasizes the distinction between employing individual IRCs versus IO as an integrating function of IRCs. Therefore, the individual employment of a single IRC may or may not be related to IO, depending upon its intended use.

1.1. IRCs are tools, techniques, or activities employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. For analytical purposes, the information environment is subdivided into the physical, informational, and cognitive dimensions. It is important to note that in addition to what are normally thought of as capabilities, IRCs may also include activities (e.g., counterpropaganda, engagements, and show-of-force) and techniques (e.g., having a partner designated as the lead for night raids or not using dogs to search houses). Although not all inclusive, the following is a list of several Air Force IRCs.

1.1.1. Intelligence, Surveillance, and Reconnaissance (ISR) in support to IO.

1.1.2. Electronic Warfare (EW) and its three sub-divisions of electronic attack (EA), electronic protection (EP), and electronic warfare support (ES).

1.1.3. Cyberspace Operations (CO) and its mission categories, including offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DoD information network (DoDIN) operations.

1.1.4. Military Deception (MILDEC)

1.1.5. Operations Security (OPSEC)

1.1.6. Military Information Support Operations (MISO)

1.1.7. Public Affairs (PA), including Combat Camera

1.1.8. Special Technical Operations (STO)

1.1.9. Counterintelligence

1.1.10. Space related capabilities

2. General. IO is not about ownership of individual capabilities, but rather the integrated and synchronized planning, monitoring, and assessment of IRCs that are then employed to create a desired effect contributing to a specified end state. IO considerations will be integrated into military strategy across the range of military operations and exercises; Air Force specialized training; communications-computer architectures and processing; information processing; doctrine, operational concepts, operational and tactical planning and execution; weapons systems research, development, testing and evaluation (RDT&E); inspections; acquisition and procurement; force development; and professional military education.

2.1. IO is inextricably linked with Command and Control (C2). C2 is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations. Similarly, IO focuses on the planning and coordination of a combination of IRCs aimed at ultimately creating effects in the cognitive dimension.

2.2. The Air Force may use an IRC by itself or in conjunction with other IRCs for the purpose of both conducting and supporting a wide range of missions. Any IRC can be a significant contributor to IO and should be taken into consideration in the planning process. Integrating IRCs to affect decision-making will be part of the normal Joint Operational Planning Process Air and/or Joint Air Tasking Cycle and will not be viewed as a separate plan or planning effort.

2.3. Proper use of IO can have a major effect in successfully meeting component and combatant command objectives. One focus of IO is to influence, disrupt, corrupt or usurp an adversary's use of information and information systems relating to C2, intelligence, and other critical information-based processes directly related to conducting military operations. A second focus of IO is to ensure themes and messages designed to influence adversaries and potential adversaries are synchronized with actions to support operational objectives. The Air Force will employ a strategy to render an adversary's information and influence efforts ineffective and create an operational advantage by effectively planning IO and appropriately employing IRCs, synchronized with allied and coalition IO. To these ends, the Air Force will:

2.3.1. Maximize United States (U.S.), allied, and coalition military effectiveness by integrating IO into military strategy, plans, operations, exercises, training, communications architectures, information processing, systems development, and professional military education while reducing friendly vulnerabilities.

2.3.2. Organize, train, and equip forces to provide IRC specialists and IO planners to combatant and component commanders, as required.

2.3.3. Implement procedures to defend the sources of friendly information that may be exploited by adversaries.

2.3.4. Maintain capabilities and procedures to identify, collect, and analyze friendly unclassified information communications to determine if any critical or classified information transmitted could adversely affect U.S. (and allied/coalition) operations.

2.3.5. Plan for IO and employ IRCs in a manner to minimize undesired interpretations of intent.

2.3.6. Ensure IO considerations are coordinated and integrated with all US, allied, and coalition planning and employment to the maximum extent practical.

2.3.7. Provide trained personnel to the joint community as part of the Joint IO force. The Joint IO force is defined as: A force consisting of units, staff elements, and individual military professionals in the Active and Reserve Components, and DoD civilian employees who conduct or directly support the integration of IRCs against adversaries and potential adversaries during military operations, as well as those who train these professionals.

2.3.8. Ensure the appropriate and systematic consideration, integration, coordination and synchronization of all planned verbal, visual, symbolic activities, and products which may be employed at the operational and tactical levels, to convey intentions, themes, and messages. This effort should support an approved combatant command and/or component theater communication strategy.

2.3.9. When reactionary IO considerations are required, such as unintended consequences of friendly actions or in response to enemy inform or influence efforts, be prepared to facilitate the response (e.g. supporting counterpropaganda efforts), as required.

2.3.10. Recognize allied and coalition partner cultural values, interests, concerns, rules of engagement, legal constraints for operating within the information environment as well as be familiar with their doctrine, tactics, techniques and procedures (TTPs). Learn these as early in the process as possible in order to maximize the sharing of information so that an integrated and achievable IO strategy can be developed and implemented throughout the operation. Allied and coalition partner cultural expertise is critical to knowing the audience for cognitive affect, whether that be change or sustainment of behavior.

3. Responsibilities. This directive establishes the following responsibilities and authorities:

3.1. The Deputy Chief of Staff for Operations, Plans and Requirements (AF/A3/5) will serve as the office of primary responsibility (OPR) for oversight of Air Force IO doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF-P) considerations. The AF/A3/5 will serve as the senior Air Force IO officer and representative. AF/A3/5 is responsible for integrating PA activities focused on adversaries and potential adversaries. Other offices having responsibilities for IRCs will coordinate with AF/A3/5 to ensure the consistent and standardized application of IO strategic planning, policy, guidance, and programmatic oversight.

3.1.1. AF/A3/5 will delegate IO OPR responsibilities to the Director of Irregular Warfare (AF/A3O-Q). AF/A3O-Q will:

3.1.1.1. Oversee the operation of an AF Integrated Process Team (AF IO IPT) to ensure an integrated approach in delivering effects based capabilities by linking the

Concept of Operations (CONOPS) for IO to the Warfighter, AFPD 10-7, Information Operations and serve as co-chair with Air Combat Command (ACC). The AF IO IPT ensures requirements and capabilities are integrated across the Air Force. They develop a consolidated plan that documents, validates, and prioritizes the Air Force's identified IO capabilities gaps and shortfalls, and completes a solution search across each DOTMLPF-P category.

3.1.2. The Information Operations Division (AF/A3O-QI) will serve as lead for coordinating oversight of IO DOTMLPF-P issues. All other Headquarters Air Force (HAF) offices with IRC responsibilities will coordinate with AF/A3O-QI on policy and guidance related to IO matters which direct the integrated employment of IRCs. This coordination requirement excludes DOTMLPF-P issues related to individual IRCs (e.g. CO, EW and ISR). To this end, AF/A3O-QI will:

3.1.2.1. Be responsible for all Air Force IO-related policy, guidance, strategy, and investment priorities.

3.1.2.2. Be responsible for oversight of IO training for IO force personnel, as well as general IO training for all Airmen.

3.1.2.3. Serve as the OPR for the Air Force portion of the analysis and findings to the Under Secretary of Defense for Intelligence (USD[I]) and the Chairman of the Joint Chiefs of Staff, on accession, retention and promotion rates of the IO force.

3.1.2.4. Coordinate all programmatic actions related to IO with Deputy Chief of Staff for Strategic Plans and Programs (AF/A8), or other panel chairs as appropriate, and submit required changes through the Air Force Corporate Structure (AFCS) in accordance with (IAW) AFI 16-501.

3.1.2.4.1. Ensure IO requirements and capabilities are integrated across the Air Force.

3.1.2.5. Serve as the Functional Manager for Air Force designated IO force positions.

3.1.2.5.1. In coordination with IRC career field managers (CFMs), AF/A3O-QI will be responsible for development and management of the IO force.

3.1.2.5.2. Coordinate with the Deputy Chief of Staff, Manpower, Personnel and Services (AF/A1) and IRC Functional Managers (FMs) and Development Teams to ensure assignment of their respective personnel, as available, to appropriate IO positions making use of IO SEIs and the U-Prefix to the maximum extent possible.

3.1.2.5.3. Coordinate with AF/A1, Air Force Personnel Center (AFPC), and CFMs to develop and maintain a baseline of IO positions and an automated capability to identify and track Air Force and Joint IO billets and personnel with IO experience.

3.1.2.5.4. Coordinate with AF/A1, AFPC, and CFMs to establish or supplement current professional development boards to monitor accession, training, education and career development for the IO force.

3.1.2.5.5. Coordinate with AF/A1, AFPC, and CFMs to establish education,

training, and experience standards.

3.1.2.5.6. Develop and implement procedures that provide appropriate oversight of education, training, and career development opportunities for members of the IO force.

3.1.2.6. Coordinate with appropriate HAF, ACC, Air Force Materiel Command (AFMC), Air Force Special Operations Command (AFSOC), Air Force Space Command (AFSPC), Air Force Global Strike Command (AFGSC), and Air Mobility Command (AMC) organizations to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.1.2.7. Ensure an IPT is formed to help steer IO in the Air Force.

3.1.2.8. Participate as a co-chair of the AF IO IPT to ensure requirements and capabilities are integrated across the Air Force.

3.2. The Director of Operational Capability Requirements (AF/A5R) will participate in the AF IO IPT to ensure requirements and capabilities are integrated across the Air Force.

3.3. The Office of the Secretary of the Air Force, Directorate of Public Affairs (SAF/PA) will serve as OPR for PA operations and participate in the AF IO IPT to ensure PA requirements and capabilities are integrated across the Air Force.

3.4. The Office of the Secretary of the Air Force, Information Dominance and Chief Information Office (SAF/CIO A6) will:

3.4.1. Participate in the AF IO IPT to ensure technical integration is addressed for the Air Force enterprise.

3.4.2. Coordinate with other appropriate HAF elements, ACC, AFMC, AFSOC, AFSPC, AFGSC, and AMC to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.4.2.1. Ensure integration of Combat Air Forces (CAF), Special Operation Forces (SOF), and Mobility Air Forces (MAF) IO TTPs.

3.5. The Deputy Chief of Staff for Intelligence (AF/A2), as the lead for AF ISR DOTMLPF-P, will:

3.5.1. Participate in the AF IO IPT to ensure intelligence requirements and capabilities are integrated across the Air Force.

3.5.2. Coordinate with other appropriate HAF elements, ACC, AFMC, AFSOC, AFSPC, AFGSC, and AMC to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.6. The Assistant Secretary of the Air Force, Acquisitions (SAF/AQ) will serve as the OPR for the RDT&E of Air Force IO acquisition activities, to include providing direction, guidance and supervision over all matters pertaining to the formulation, review, approval and execution of plans, policies, and programs relative to research, development, production and acquisition of IO programs and defense materiel. SAF/AQ will:

3.6.1. Participate in the AF IO IPT to ensure IRC requirements and capabilities are integrated across the Air Force.

- 3.6.2. Coordinate with the AF IO IPT to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.
- 3.6.3. Create, coordinate, and represent appropriate IO funding justification IAW decisions made by the AFCS for the Air Force, DoD and Congress, to include management of funds allocated for acquisition programs within the RDT&E appropriation.
- 3.6.4. Ensure that the AF IO IPT is well informed of all relevant RDT&E efforts throughout the Air Force and other DoD and National Agencies.
- 3.7. The Deputy Chief of Staff, Manpower, Personnel, and Services (AF/A1) and AFPC, in coordination with AF/A3O-QI and CFMs, will:
- 3.7.1. Develop a baseline of IO positions and an automated capability to identify and track Air Force IO billets and personnel, as well as the IO force.
- 3.7.2. Document education, training, and experience standards for the IO force.
- 3.7.3. Assign skilled and qualified personnel to IO positions making use of IO SEIs and the U-Prefix to the maximum extent possible.
- 3.7.4. Establish or supplement current professional development boards to monitor accession, training, education and career development for the IO force.
- 3.8. The Office of the General Counsel, Division of International Affairs (SAF/GCI) ensures all Air Force applications of IRCs are consistent with U.S. policy and law.
- 3.9. Air Combat Command, as the lead command for IO, has IO responsibilities and authorities at the Air Force, CAF and Major Command (MAJCOM) level as directed in AFPD 10-9, Lead Command Designation and Responsibilities for Weapon Systems. ACC is also the lead command for the MILDEC, OPSEC, MISO, and EW IRCs. Any agreement between ACC and another MAJCOM to delegate roles or responsibilities will be outlined in a Memorandum of Agreement between the two and a copy will be provided to AF/A3O-QI. To that extent, ACC will:
- 3.9.1. Coordinate with other MAJCOMs and consolidate input on funding requirements, justification, and out-year strategy. Provide inputs to AF/A3O-QI to support planning and programming for IO.
- 3.9.1.1. Execute IO funding in accordance with spend plan.
- 3.9.1.2. Organize, train, and equip IO forces and capabilities, to include readiness assessment and evaluation functions, and leading integration of IO into all CAF-mission areas.
- 3.9.1.3. Work issues to include establishing and integrating IO within the Air Force Forces (AFFOR) and AOC; consolidate/ integrate IO into theater air operations; and standardize CAF IO organization and be responsible for the formation, manning, and training of IO forces.
- 3.9.1.4. Act as the primary functional manager, training manager, syllabus review and registrar responsibilities for IO and the OPSEC and MILDEC courses.

- 3.9.1.5. Serve as OPR for course content and standards for all Air Force IO Initial Qualification Training (IQT), CAF Mission Qualification Training (MQT) and continuation training for IO forces.
- 3.9.1.6. Lead development of training for capability specialists to conduct IO tactics, techniques, and procedures and operational level planners to apply the doctrine and tenets of Air Force IO within the Air and Space Operations Centers (AOCs).
- 3.9.1.7. Provide updated IO training course information to the Joint Training Course Database according to Joint Staff guidance.
- 3.9.1.8. Include IO in CAF-sponsored and supported exercises, as appropriate.
- 3.9.1.9. Serve as OPR for the development of all Air Force IO enabling concepts, Operational-TTP's, with assistance from AFSPC, and for the assessment of IRCs, including against potential threats.
- 3.9.1.10. Be responsible for all functions related to defining, documenting, advocating, programming, and directing the transformation, modernization, sustainment, upgrade, and testing of CAF IO systems and programs.
- 3.9.1.11. Define CAF IO operational requirements.
- 3.9.1.12. Maintain CAF IO readiness and resolve related issues.
- 3.9.1.13. Serve as the CAF interface with the HQ Air Force staff and other agencies for IO modernization interoperability.
- 3.9.1.14. Advocate and monitor for CAF IO modernization needs and solutions.
- 3.9.1.15. Charter and establish the supporting structure in order to develop the AF IO IPT and ensure its products are integrated into the Air Force strategic planning process. ACC will serve as co-chair of the AF IO IPT with AF/A3O-Q and be the Office of Collateral Responsibility (OCR) for the AF IO IPT.
- 3.9.1.16. Ensure all Air Force commands, organizations, and agencies will use the AF IO IPT when addressing IO shortfalls. The AF IO IPT will collect, assess, prioritize, and advocate for IO solutions to be included in Program Objective Memorandum using the appropriate Program Element Codes (PECs).
- 3.9.2. Coordinate with the AF IO IPT to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.
- 3.9.3. Assist and support Air Staff in the performance of their DOTMLPF-P responsibilities, as required.
- 3.9.4. Perform reachback targeting support for IO and operations focused on influence of foreign audiences, via the Air Force Targeting Center.
- 3.10. Air Mobility Command is the lead for IO at the MAF. AMC will:
 - 3.10.1. Support the MAF integration into the Air Force strategic planning process.
 - 3.10.2. Organize, train and equip MAF IRCs to include assets supporting IO conducted by MAF organizations. AMC will lead centralized management of MAF IRCs; establish and integrate IO in the 618 AOC (TACC); coordinate specialized IO related

requirements; consolidate/integrate MAF IO requirements into theater air operations; standardize MAF IO organization, training and equipment; and integrate MAF special access programs into operations and exercises. AMC will:

3.10.2.1. Serve as MAF OPR for the development of OTTPs and for the assessment of IRCs.

3.10.2.2. Serve as OPR for planning, coordinating, and conducting MQT for MAF IO forces.

3.10.2.3. Coordinate with the AF IO IPT to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.11. Air Force Special Operations Command will:

3.11.1. Coordinate with the AF IO IPT to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.11.2. Organize, train and equip SOF IRCs to include assets supporting IO conducted by SOF organizations. AFSOC will lead centralized management of SOF IRCs; establish and integrate IO in the Joint Special Operations Air Component (JSOAC); coordinate specialized IRCs; consolidate requirements into SOF air operations; and integrate SOF special access programs into operations and exercises.

3.11.2.1. Serve as OPR for planning, coordinating, and conducting qualification training for assigned IO forces.

3.11.2.2. Serve as SOF OPR for the development of TTPs and for the assessment of IO capabilities.

3.11.2.3. Coordinate with appropriate Air Staff and MAJCOM IO offices on all exercise and training requirements for IO personnel.

3.12. Air Force Materiel Command (AFMC) will:

3.12.1. Coordinate with the AF IO IPT to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.12.2. Provide the subject matter expertise necessary to assist the Air Force Life Cycle Management Center (AFLCMC), the Program Managers, and AOCs to explore alternative developmental courses of action for new IRCs, as well as ensuring integration of IO into weapon systems' RDT&E.

3.12.3. Ensure that IO mid-term and long-term research and technology shortfall issues are adequately addressed through Air Force Research Laboratory activities, and advocate for solutions.

3.12.4. Ensure that the AF IO IPT is well informed of all relevant RDT&E efforts throughout the Air Force.

3.12.5. Educate MAJCOMs, Combatant Commands (CCMDs), Component Numbered Air Forces, and AOCs on intelligence capability for support of intelligence acquisition requirements with the appropriate offices/agencies.

3.13. Air Education and Training Command (AETC) will:

3.13.1. Implement the approved life-cycle strategy, as defined by the Air Force IO Training Planning Team (TPT), which defines total force education and training needed to satisfy mission-generated IO requirements.

3.13.2. Participate in and chair, when appropriate, Utilization and Training Workshops (U&TWs) and TPTs, which address IO training requirements for the core Air Force Specialty Codes (AFSCs) that feed the IO force.

3.14. Air Force Space Command, as lead command for Air Force cyberspace capabilities, AFSPC will:

3.14.1. Serve as OPR for planning, coordinating, and conducting training for AFSPC IO forces.

3.14.2. Coordinate with the AF IO IPT to incorporate Air Force IO initiatives into Joint/Air Force experimentation and acquisition activities.

3.14.3. Advance AF IO, MISO, MILDEC, OPSEC, capabilities in collaboration with U.S. Government national level agencies and organizations, i.e. DoD, Interagency OPSEC Support Staff, etc, in the National Capital Region.

3.14.4. Support development of Air Force IO capabilities.

3.14.5. Plan and participate in AF and Joint exercises for the purpose of capturing and evaluating IO, MISO, MILDEC, and OPSEC Tactics, Techniques, and Procedures.

3.14.6. Test and evaluate emerging IO, MISO, MILDEC, OPSEC, and offensive and defensive cyberspace capabilities for operational forces, national agencies, and the acquisition community.

3.14.7. Provide IO, MISO, MILDEC, and OPSEC initial and advanced qualification training instruction for the Air Force as directed.

3.14.8. Be Office of Primary Responsibility (OPR) for all IO force courses for which 39th Information Operations Squadron (IOS) and 229th IOS are designated as the Office of Primary Development Responsibility (OPDR). This includes all current and any future IO force courses.

3.14.9. Develop IO, MISO, MILDEC, OPSEC, tactics, techniques, and procedures for joint and AF operational planners in support of current and future operations.

3.14.10. Provide support to IO, MISO, MILDEC, OPSEC, planning and assessment conducted by Numbered Air Forces and MAJCOMs.

3.14.11. Provide IO, MISO, MILDEC, OPSEC process and tool assessments and document/refine IO requirements and operational architectures.

3.14.12. Provide and support IO education and training for the total force, employing advanced distributed learning (ADL) and instructors.

3.14.13. Ensure IO courses are created in accordance with the Air Force Instructional System Development (ISD) process.

3.14.14. Coordinate on all IO, MISO, MILDEC, and OPSEC Task Training Lists (TTL) and training syllabi; Tactics, Techniques, and Procedures (TTP) development; exercise support; and reachback support requirements.

3.14.15. AFSPC will coordinate and assist ACC, other component MAJCOMS, and component Numbered Air Forces (NAF) with:

3.14.15.1. Operation of the AF IO training unit providing Airmen with technical, tactical, and operational skills required to plan missions and operate AF IO, MISO, MILDEC, and OPSEC capabilities for operational forces, national agencies, and the acquisition community.

3.14.15.2. Prioritization of IO-related education and training efforts.

3.14.15.3. Providing personnel support and funding of AFSPC IO forces for exercises.

3.14.15.4. Production of IO white papers and concepts.

3.14.15.5. The support of air, space, cyber and IO ranges.

3.14.15.6. Supporting reachback requests for all Air Force IO, MISO, MILDEC, and OPSEC personnel.

3.14.15.7. AOC IOTs efforts through reachback capabilities and support to include, but not limited to: planning; strategy development and analysis; targeting and weaponeering; synchronization of kinetic and non-kinetic activities; and assessments.

3.14.15.8. Development and delivery of Air Force IRCs that disrupt, corrupt, and usurp adversarial decision making while protecting our own.

3.14.15.9. Integrating IO, MISO, MILDEC, and OPSEC capabilities, planning and execution into the Mobility Air Forces' and Combat Air Forces' training and exercises at the operational and tactical levels."

3.14.15.10. Conducting the Information Operations Integration Course (IOIC), and other IO force training to ensure AOC Information Operations Team (IOT) requirements are being fulfilled.

3.14.15.11. Supporting the Air Force Warfare Center (USAFWC) with IO expertise for training and exercises.

3.15. National Air and Space Intelligence Center (NASIC) will support AFFOR and AOC IO and influence efforts, to include, but not limited to support via behavioral influence analysis.

3.16. All MAJCOMs, FOAs, DRUs, Air Force Reserve Command (AFRC) and the Air National Guard (ANG) will:

3.16.1. Develop IO programs and policies aligned with Air Force IO program and policy guidance issued by AF/A3/5 and ensure subordinate organizations integrate applicable IRCs into day-to-day operations.

3.16.2. Be responsible for actively participating in and supporting the AF IO IPT.

3.16.3. Use established requirements procedures and documentation, such as Initial Capabilities Documents, Capability Development Documents, inputs to the combatant commanders' Integrated Priority Lists and Joint Requirements Oversight Council reviews, Quadrennial Defense Reviews, lessons learned, and ad hoc studies to identify and document IO requirements and deficiencies, and to provide those inputs to the AF IO IPT in accordance with guidance. Also submit potential solutions for vetting, visibility, and advocacy among all AF IO IPT members.

3.16.4. When specifically authorized by HAF, organize, train and equip assigned IO forces. IO units shall not be created nor will existing units become IO units, without specific authorization from HAF.

3.16.5. Coordinate with AFRC/ANG on matters pertaining to total force integration with IO requirements.

3.16.6. Plan and participate in AF and joint exercises for the purpose of capturing and evaluating IO, MISO, MILDEC, and OPSEC TTPs as applicable.

3.17. In coordination with AF/A3/5 and other appropriate agencies, AFFOR and AOC commanders are responsible for IO implementation, posture and operations within their commands and units.

4. See [Attachment 1](#) for references and supporting information.

DEBORAH LEE JAMES
Secretary of the Air Force

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

DoD, National Defense Strategy, June 2008

DoD Directive (DoDD) 3600.01, Information Operations (IO), 2 May 2013

DoDD 5205.02E, DOD Operations Security (OPSEC) Program, 20 June 2012

DoDD 5240.01, Change 1, DoD Intelligence Activities, 29 January 2013

DoDD 8500.01E, Information Assurance, 24 October 2002

DoDD O-8530.1, Computer Network Defense (CND), 8 January 2001

DoD Instruction (DoDI) 3604.01, DoD Military Deception, 11 March 2013

DoDI 3608.11, Information Operations Force Development, 4 November 2005

DoDI 8560.01, Communications Security (COMSEC) Monitoring & Information Assurance (IA) Readiness Testing, 9 October 2007

CJCS, National Military Strategy, January 2012

CJCS Instruction (CJCSI) 3170.01F, Joint Capabilities Integration and Development System (JCIDS), 10 Jan 2012

CJCSI 3210.01B, Joint Information Operations Policy (U), 13 January 2010

CJCSI 3211.01D, Joint Policy for Military Deception, 1 August 2007

CJCSI 3213.01C, Joint Operations Security, 17 July 2008

CJCSI 3320.01D, Joint Electromagnetic Spectrum Operations (JEMSO), 21 Jan 13

CJCSI 6212.01E, Interoperability and Supportability of Information Technology & National Security Systems, 15 December 2008

CJCSI 6510.01F, Information Assurance (IA) and Computer Network Defense (CND), 09 February 2010

CJCS Manual (CJCSM) 1630.01, Joint Information Operations Force, 16 March 2009, (CAO 16 May 11)

Joint Publication (JP) 1-02, Amended, DoD Dictionary of Military & Associated Terms, 31 January 2011

JP 3-13, Information Operations, 27 November 2012

Air Force Doctrine Volume IV, Operations; Chapter 3, A Review of Air Force Operations; Annex 3-13, Information Operations, 29 October 2013

AFPD 10-6, Capabilities-Based Planning & Requirements Development, 31 May 2006

AFPD 10-9, Lead Command Designation & Responsibilities for Weapons Systems, 8 March 2007

AFPD 10-17, Cyberspace Operations, 31 July 2012
AFPD 33-2, Information Assurance Program, 03 August 2011
AFPD 33-3, Information Management, 08 September 2011
AFPD 35-1, Public Affairs Management, 28 September 2012
AFPD 71-1, Change 2, Criminal Investigations and Counterintelligence, 30 September 2011
AFI 10-601, Capabilities Based Requirements Development, 12 July 2010
AFI 10-701, Operations Security (OPSEC), 8 June 2011
AFI 10-702, Military Information Support Operations (MISO), 7 June 2011
AFI 10-703, Electronic Warfare Integrated Reprogramming, 19 October 2010
AFI 10-704, Military Deception Program, 30 August 2005
AFI 10-706, Electronic Warfare (EW) Operations, 30 November 2007
AFI 10-707, Spectrum Interference Resolution Program, 20 June 2005
AFI 14-104, Oversight of Intelligence Activities, 23 April 2012
AFI 16-501, Control and Documentation of Air Force Programs, 15 August 2006
AFI 33-115V1, Network Operations (NETOPS), 24 May 2006
AFI 35-101, Public Affairs Responsibilities and Management, 18 August 2010
AFI 71-101V4, Counterintelligence, 8 November 2011
AFMAN 33-363, Management of Records, 1 March 2008
Air Force Interim Computer Network Attack (CNA) Security Classification Guide, 3 June 2002
(Classified: contact AF/A3C/A6C)
Air Force Military Deception Security Classification Guide, 15 March 2011 (Classified: contact
AF/A3O-QI)

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*, 22 Sep 09.

Abbreviations and Acronyms

ACC—Air Combat Command
AETC—Air Education and Training Command
AFCS—Air Force corporate structure
AFDD—Air Force doctrine document
AFFOR—Air Force Forces
AFI—Air Force instruction
AFLCMC—Air Force Life Cycle Management Center
AFMAN—Air Force manual

AFMC—Air Force Materiel Command

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force policy directive

AFRC—Air Force Reserve Command

AFSC—Air Force specialty code

AFSOC—Air Force Special Operations Command

AFSPC—Air Force Space Command

AFWC—Air Force Weapons Course

AMC—Air Mobility Command

ANG—Air National Guard

AOC—air and space operations center

C2—command and control

CAF—Combat Air Force

CCMD—Combatant Commands

CFM—career field manager

CI—counterintelligence

CJCS—Chairman, Joint Chiefs of Staff

CO—cyberspace operations

CSAF—Chief of Staff of the Air Force

DCO—defensive cyberspace operations

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DOTMLPF—P —doctrine, organization, training, materiel, leadership and education, personnel and facilities policy

DRU—direct reporting unit

EW—electronic warfare

FOA—field operating agency

HAF—Headquarters Air Force

HQ—headquarters

AF/A1—Deputy Chief of Staff, Manpower, Personnel and Services

AF/A2—Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance

AF/A3/5—Deputy Chief of Staff, Operations, Plans, and Requirements

AF/A3C/A6C—Director of Cyberspace Operations
AF/A3O—Q —Irregular Warfare Directorate
AF/A3O—QI —Information Operations Division
AF/A3S—Director of Strategic Security
AF/A5R—Director of Operational Capability Requirements
AF/A5X—Director of Operational Plans and Joint Matters
IA—information assurance
IAW—in accordance with
IO—information operations
IPT—integrated process team
IRC—information related capabilities
IQT—initial qualification training
ISR—intelligence, surveillance, and reconnaissance
JP—joint publication
MAF—Mobility Air Force
MAJCOM—Major Command
MILDEC—military deception
MISO—military information support operations
MQT—mission qualification training
NAF—Numbered Air Force
OCO—offensive cyberspace operations
OCR—office of collateral responsibility
OPR—office of primary responsibility
OPSEC—operations security
OTTP—operational tactics, techniques, and procedures
PA—public affairs
RDT&E—research, development, testing and evaluation
SAF/AQ—Secretary of the Air Force, Acquisitions
SAF/CIO A6—Directorate for Information Dominance, Chief Information Officer
SAF/IG—Secretary of the Air Force, Inspector General Office
SAF/PA—Secretary of the Air Force, Office of Public Affairs
SEI—special experience identifier

TMAP—Telecommunications Monitoring Assessment Program

TPT—training planning team

TTP—tactics, techniques and procedures

US—United States

U&TW—utilization and training workshop

Terms

Counterintelligence (CI)—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (AFDD 3-13; JP 1-02)

Cyberspace Operations—The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-12)

Functional Manager—The authority responsible for policy and procedures associated with systems within a given functional area.

Information—1) Facts, data, or instructions in any medium or form. 2) The meaning that a human assigns to data by means of the known conventions used in their representation. (AFDD 3-13; JP 1-02)

Information Environment— The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

Information Related Capability—Capabilities, techniques, and activities employed within a dimension of the information environment that can be used to achieve a specific end(s). (JP 3-13)

Information Assurance (IA)—Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP 3-13)

Information Operations (IO)—The integrated employment, during military operations, of **information**—related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own. (JP 3-13)

Information Operations Force (IO force)—A force consisting of units, staff elements, and individual military professionals in the Active and Reserve Components, and DoD civilian employees who conduct or directly support the integration of IRCs against adversaries and potential adversaries during military operations as well as those who train these professionals. (DoDD 3600.01)

Information System—The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. (JP 3-13)

Intelligence, Surveillance, and Reconnaissance (ISR)—Intelligence, surveillance, and reconnaissance are integrated capabilities to collect, process, exploit, and disseminate accurate

and timely information that provides the battlespace awareness necessary to successfully plan and conduct operations. (AFDD 3-13; AFDD 2-0)

Military Deception (MILDEC)—Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly forces mission. (AFDD 3-13; JP 1-02) [There are five categories of military deception. See JP 1-02 for the complete definition.]

Military Information Support Operations (MISO)—Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. (JP 3-13.2)

National Capital Region (NCR)— A geographic area encompassing the District of Columbia and eleven local jurisdictions in the State of Maryland and the Commonwealth of Virginia. (JP 1-02)

Operations Security (OPSEC)—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a) identify those actions that can be observed by adversary intelligence systems; b) determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (AFDD 3-13; JP 1-02)

Public Affairs (PA)— Those public information, command information, and community engagement activities directed toward both the external and internal audiences with interest in the Department of Defense (JP 1-02; JP 3-61). Through the release of timely, truthful, and accurate information and imagery, PA puts operational actions in context, facilitates development of informed perceptions about military operations, and helps undermine adversary propaganda.

Total Force—The entire range of organizational roles and responsibilities that comprise the active duty Air Force, Air Force Reserve and Air National Guard.